

FILE: 70-7 85-3365

ROUTING AND RECORD SHEET

SUBJECT: (Optional)

Agency comments to ISOO on new information security initiatives.

FROM: [Redacted] Office of Information Services 1236 Ames Building		EXTENSION	NO.	STAT
			DATE 27 September 1985	STAT
TO: (Officer designation, room number, and building)	DATE	OFFICER'S INITIALS	COMMENTS (Number each comment to show from whom to whom. Draw a line across column after each comment.)	
	RECEIVED	FORWARDED		
1. EO/DDA	27 SEP 1985	EM	[Redacted] STAT	
2. ADDA	27 SEP 1985	J	<p>On 30 July 1985, the Information Security Oversight Office (ISOO) established five task forces to identify new initiatives in the information security area. On 3 September, D/ISOO forwarded for our review and comment the papers submitted to ISOO by the task forces. The issues we are commenting on are: unauthorized disclosures, overclassification, need to know and classification management.</p>	
3.				
4.				
5.				
6. DDA/INFO	30 SEP 1985	EM		
7.			<p>Attached are our comments (and some background). They have been coordinated with the DCI Security Committee, O/Security, O/General Counsel and O/Personnel.</p>	
8.			<p>[Redacted] directed that they be sent to you for O/DDA information/concurrence. STAT</p>	
9.			<p>Our deadline is 30 September and, unless you see a problem, we will pass them to ISOO Monday morning. If at all possible, I would appreciate a call this afternoon.</p>	
10. DDA Registry			<p>My apologies for the short deadline. STAT</p>	
11.			<p>Thank you.</p>	
12.			<p>STAT</p>	
13.			<p>[Redacted]</p>	
14.			<p>I phoned [Redacted] 1550 Sep 27 and said attached is OK with O/DPA and no objections to Ben releasing his reply due 30 Sep. STAT</p>	
15.			<p>[Redacted]</p>	

I. UNAUTHORIZED DISCLOSURES

1. Initiative - Identify proposed legislation/regulations concerning the implementation of NSDD 84 that impact on unauthorized disclosures.

We agree with the broad scope of this initiative in that legislation is needed to resolve the growing problem of unauthorized disclosures. Specifically, we concur with a mandatory minimum penalty for individuals found to have made an unauthorized disclosure of classified information. We further recommend that ISOO pursue the issue of enforcing the reporting requirement in Executive Order 12333, 1.7 (a) & (b), that senior officials of intelligence agencies report possible violations of federal criminal laws or serious breaches of security to the Attorney General and that these cases be referred to the FBI for further investigation.

2. Initiative - Develop educational media concerning unauthorized disclosures to increase awareness among Government employees.

Increased awareness of the seriousness of unauthorized disclosures on the part of every Government employee and is a prerequisite to a strong security system. We support the theme of this initiative and recommend that ISOO take the lead in developing specific educational training aids for use by all Government agencies and departments.

This initiative refers to several proposals by the CIA for classified videotapes on leaks. The CIA presently does not have any proposals under consideration for such tapes. However, the DCI Security Committee (SECOM) is now in the process of contracting for the script of a videotape on unauthorized disclosures including the resulting damage of such disclosures. When the tape is completed it will be made available for use by other Government agencies probably as part of a SECOM program. Unfortunately, the need to show the cause-and-effect relationship between disclosures and the resulting damage precludes the possibility that this videotape will be available in an unclassified format.

-2-

3. Initiative - Develop programs to encourage the reporting of unauthorized disclosures e.g., set up a toll-free hotline.

We heartily endorse ISOO exploring the merits of any proposal or legislation aimed at stemming the flow of classified information by unauthorized disclosures. However, we suggest that the success of the DOD hotline first be evaluated to determine its effectiveness before establishing a "civilian" hotline system.

Contrary to the statement contained in this initiative, the CIA has not initiated a proposal to establish rewards for the reporting of unauthorized disclosures.

4. Initiative - Revise investigative procedures and security inspections pertaining to unauthorized disclosures.

We endorse the recommendation that all Government agencies develop their own internal guidelines for the investigation of unauthorized disclosures. ISOO should provide guidance and assistance to those agencies or departments that have not yet developed such guidelines or that require assistance in revising outdated guidelines. As stated in Initiative 1., we encourage the enforcement of Executive Order 12333, 1.7 (a) & (b), concerning the reporting of violations to the Attorney General and the FBI.

II. OVERCLASSIFICATION

1. Initiative - Establishment by the ISOO of minimal criteria for mandatory training for classifiers.

As stated in this initiative, Executive Order 12356 and the ISOO Implementing Directive already require agencies that create and handle classified information to conduct a security education program. We see no need to expand on this requirement nor do we feel that detailing minimal standards would be a practical or useful exercise. We agree that education and training programs vary widely among agencies. However, because the individual needs of government agencies and departments vary to such a great extent, their individual training requirements are also quite different. We suggest that ISOO place additional emphasis on security education during its annual inspection program and that special assistance be provided to agencies when requested.

2. Initiative - Establishment by ISOO of criteria for determining when formal written classification guidance is required and a handbook for preparing classification guidance.

Executive Order 12356, Sec 2.2, requires agencies with original classification authority to prepare classification guides and that ISOO be notified of any waivers of this requirement. Given the fact that agency requirements for classification guides differ, we believe it is the exceptions that should be addressed rather than trying to redefine the entire system. Agencies that have special problems in developing classification guides or have a unique requirement that cannot be resolved internally should request ISOO assistance. The preparation of a handbook on how to prepare a classification guide will be of limited value at best.

3. Initiative - Establishment by ISOO of minimal criteria for agency self-inspections, ISOO inspections, and agency review for overclassification.

Executive Order 12356, Sec 5.2 (4) and the ISOO Implementing Directive 2001.62 already establishes a minimal standard for agency and ISOO inspections. Although we agree that overclassification is an important concern, the most effective means of preventing this problem is through the use of detailed classification guides and the application of standard procedures for reviewing documents at the time of origination. Agency heads should be responsible for determining their own standards for periodic self-inspections.

4. Initiative - Provide an effective means for classification decisions to be challenged by those who believe a document is overclassified and impose a requirement on Executive Branch employees to challenge the classification of documents believed to be overclassified.

Neither Executive orders nor ISOO directives can cover every conceivable scenario dealing with improper or excessive classification decisions. Every government employee with authorized access to classified information has, at the very least, a moral obligation to question improper or overclassification of a document. Any individual who feels a document is improperly classified should first discuss the matter with the originator of the document. Failing all internal appeals, Executive Order 12356, Sec 5.2, (b) (6) provides that the Director, ISOO shall consider and take action on complaints and suggestions from persons within or outside the Government with respect to the administration of the information security program.

III. NEED-TO-KNOW

1. Initiative - Propose a vigorous campaign, possibly initiated by a statement from the White House, under the general responsibility of ISOO but centered in the Senior Official in each agency, to remind all classifying officers of their responsibility in applying the need-to-know principle.

We enthusiastically support this initiative.

2. Initiative - Agencies which are able to control access to limited bodies of information should continue to do so and all agencies should examine their procedures to see if other limited area control can be achieved.

We concur in this initiative and suggest that ISOO consider monitoring the progress of this initiative during its annual inspection program.

3. Initiative - Agencies should, wherever possible, establish a spot-checking procedure for documents to determine the appropriateness of classification.

We concur with spot-checking wherever possible. However, the use of classification guides and standard review procedures at the time of origination is considered a more effective routine method for determining the correctness of classification levels.

4. Initiative - Some redrafting of Executive Order 12356 and/or the ISOO directive may be necessary in order to accommodate new procedures and legitimate concerns.

We consider this initiative unnecessary. Executive Order 12356 and the ISOO implementing directive provide sufficient justification for acting on the initiatives proposed by the various task forces. Implementation of the initiatives is, for the most part, at the discretion of the senior agency official.

IV. CLASSIFICATION MANAGEMENT

1. Initiative - The President direct OPM to revise the GS-080 series, ensuring that classification management and other security functional areas are addressed as separate areas of security specialization.

We have been advised that the Security Administration Series, GS-080 (Classification & Qualification Standards) was revised in 1983 and circulated to Federal agencies for review and comment. We suggest that ISOO make inquiries to the Office of Personnel Management to determine the status of GS-080.

2. Initiative - The President direct the Secretary of Defense to explore the feasibility of expanding the Defense Security Institute to provide basic security training to personnel throughout the Executive Branch on a cost - reimbursable basis.

We do not believe that Presidential involvement in this matter is necessary. However, we do concur in expanding the Defense Security Institute for basic security training.

3. Initiative - The President revise Executive Order 12356 to identify classification management as an area warranting agency head attention.

Executive Order 12356, Sec 5.3 (a) already requires agency heads to designate a senior agency official to direct and administer its information security program. In addition, the 1983 revision of the GS-080 occupational series statement contains a detailed description for an Information Security Specialist which, if approved, will allow agency heads to upgrade or expand their information security program as necessary.